

1 Claims 1, 5, 11-13, 16, 37, 41 and 42 are amended.

2 Claims 17 and 18 are canceled.

3 Claims 1-16 and 19-42 remain in the application and are listed just below:

5 1. (Currently Amended) A method of updating keys that decrypt login
6 tickets that log a user into multiple sites, the method comprising:

7 generating a first key having a first version number;

8 providing tickets encoded consistent with the first key, the ticket having a
9 version number corresponding to the first version number;

10 generating a second key having a second version number; and when the
11 second key becomes current at a site, providing tickets encoded consistent with the
12 second key, the ticket having a version number corresponding to the second version
13 number;

14 wherein said tickets are configured to enable a user to access and use one or
15 more affiliated servers without requiring any additional authentication information
16 other than authentication information originally provided by the user to an
17 authentication server.

18
19 2. (Original) The method of claim 1 wherein a different key is provided
20 to each site, and wherein each key is encrypted for decoding at one site.

21
22 3. (Original) The method of claim 1 and further including generating a
23 configuration file to track keys for each site.

1 4. (Original) The method of claim 1 wherein the key comprises key data
2 and executable code for decrypting tickets.

3
4 5. (Currently Amended) A computer readable medium having
5 instructions stored thereon for causing a computer to perform a method of updating
6 keys that decrypt login tickets that log a user into multiple sites, the method
7 comprising:

8 generating a first key having a first version number;
9 providing tickets encoded consistent with the first key, the ticket having a
10 version number corresponding to the first version number;
11 generating a second key having a second version number; and
12 when the second key becomes current at a site, providing tickets encoded
13 consistent with the second key, the ticket having a version number corresponding to
14 the second version number;
15 wherein said tickets are configured to enable a user to access and use one or
16 more affiliated servers without requiring any additional authentication information
17 other than authentication information originally provided by the user to an
18 authentication server.

19
20 6. (Original) A method of generating keys that decrypt login tickets that
21 log a user into multiple sites, the method comprising:

22 generating a first key in the form of an executable having a first version
23 number;
24 generating a second key in the form of an executable having a second version
25 number; and

1 providing an indication to a login server identifying which key is current for
2 each site such that the tickets are properly encoded.

3

4 7. (Original) The method of claim 6 and further comprising distributing
5 the key to multiple login servers in a secure manner.

6

7 8. (Original) The method of claim 6 and further comprising updating a
8 configuration file to track keys for each site.

9

10 9. (Original) A computer readable medium having instructions stored
11 thereon for causing a computer to perform a method of generating keys that decrypt
12 login tickets that log a user into multiple sites, the method comprising:

13 · generating a first key in the form of an executable having a first version
14 number;

15 · generating a second key in the form of an executable having a second version
16 number; and

17 providing an indication to a login server identifying which key is current for
18 each site such that the tickets are properly encoded.

19

20 10. (Original) A system that generates keys that decrypt login tickets that
21 log a user into multiple sites, the system comprising:

22 · a key generator that generates a first key in the form of an executable having a
23 first version number and generates a second key in the form of an executable having
24 a second version number; and

1 means for providing information to a login server identifying which key is
2 current for each site such that the tickets are properly encoded.

3

4 11. (Currently Amended) A method of updating keys that decrypt login
5 tickets that log a user into multiple sites, the method comprising:

6 generating a new key with an incremented version number;
7 sending the new key to a partner site for use in decoding tickets with the
8 incremented version number;
9 updating key and version information for a login server; and
10 generating tickets decodable by the new key when an indication that a key
11 having a previous version number has expired;

12 wherein said tickets are configured to enable a user to access and use one or
13 more affiliated servers without requiring any additional authentication information
14 other than authentication information originally provided by the user to an
15 authentication server.

16

17 12. (Currently Amended) A computer readable medium having
18 instructions stored thereon for causing a computer to perform a method of updating
19 keys that decrypt login tickets that log a user into multiple sites, the method
20 comprising:

21 generating a new key with an incremented version number;
22 sending the new key to a partner site for use in decoding tickets with the
23 incremented version number;
24 updating key and version information for a login server; and

1 generating tickets decodable by the new key when an indication that a key
2 having a previous version number has expired;

3 wherein said tickets are configured to enable a user to access and use one or
4 more affiliated servers without requiring any additional authentication information
5 other than authentication information originally provided by the user to an
6 authentication server.

7
8 13. (Currently Amended) A method of updating a key used to decrypt
9 tickets used to log into a site, the method comprising:

10 receiving an updated key with a new version number;
11 setting a time for an old current key having an old version number to expire;
12 making the updated key the current key;
13 wherein said tickets are configured to enable a user to access and use one or
14 more affiliated servers without requiring any additional authentication information
15 other than authentication information originally provided by the user to an
16 authentication server.

17
18 14. (Original) The method of claim 13 wherein the key comprises
19 executable code for making the updated key the current key.

20
21 15. (Original) The method of claim 13 and further comprising redirecting
22 users attempting to log into the site using the old current key.

1 16. (Currently Amended) A computer readable medium having
2 instructions stored thereon for causing a computer to perform a method of updating a
3 key used to decrypt tickets used to log into a site, the method comprising:

4 receiving an updated key with a new version number;

5 setting a time for an old current key having an old version number to expire;

6 making the updated key the current key;

7 wherein said tickets are configured to enable a user to access and use one or
8 more affiliated servers without requiring any additional authentication information
9 other than authentication information originally provided by the user to an
10 authentication server.

11
12 17. (Canceled).

13
14 18. (Canceled).

15
16 19. (Original) A method of managing keys used to decrypt tickets for
17 logging onto a site, the method comprising:

18 receiving a first key with a first version number;

19 encrypting the first key using a hardware address;

20 changing a current key variable to the first version number;

21 receiving a new key with an incremented version number;

22 encrypting the new key using a hardware address; and

23 identifying the new key as the current key.

1 20. (Currently Amended) Them method of claim 19 and further
2 comprising setting a time for the first key identifying when such key may no longer
3 be used.

4

5 21. (Original) The method of claim 20 wherein a user currently logged in
6 may continue to use the first key until the time expires.

7

8 22. (Original) The method of claim 20 wherein new user may only use a
9 ticket corresponding to the second key when the second key is made the current key.

10

11 23. (Original) The method of claim 20 wherein the time is set to a
12 reauthorization time determined by the site.

13

14 24. (Original) The method of claim 19 wherein a new user using a
15 previous version ticket will be redirected to obtain a ticket corresponding to the new
16 key following the new key being identified as the current key.

17

18 25. (Original) The method of claim 19 wherein the new key is identified as
19 the current key by changing the current key variable to the second version number.

20

21 26. (Original) A computer readable medium having instructions stored
22 thereon for causing a computer to perform a method of managing keys used to
23 decrypt tickets for logging onto a site, the method comprising:

24 receiving a first key with a first version number;

25 encrypting the first key using a hardware address;

1 changing a current key variable to the first version number;
2 receiving a new key with an incremented version number;
3 encrypting the new key using a hardware address; and
4 identifying the new key as the current key.

5

6 27. (Original) A method of updating keys used to decrypt tickets used to
7 log into multiple sites on a network, the method comprising:

8 generating a new key with a new version number to take the place of an old
9 key with an old version number;
10 storing the new key on a site to be logged into by a user;
11 changing a current key indication to the new key;
12 allowing current logged in users to continue using the old key; and
13 redirecting new users to a login server to obtain a ticket consistent with the
14 new key.

15

16 28. (Original) The method of claim 27 wherein the old key may be used
17 by current logged in users for a predetermined amount of time.

18

19 29. (Original) The method of claim 28 wherein the predetermined amount
20 of time is no more than a reauthorization time by which a current user is normally
21 required to provide login information.

22

23 30. (Original) The method of claim 28 wherein the predetermined amount
24 of time may be set to zero to force all current and new users to login with a ticket
25 consistent with the new key version.

1
2 31. (Original) The method of claim 27 wherein the ticket contains a
3 version number consistent with the version number of the key which can decrypt it.

4
5 32. (Original) The method of claim 27 wherein keys are encrypted by the
6 site using a hardware address, and stored by the site.

7
8 33. (Original) The method of claim 27 wherein a new key is generated
9 based on a request of the site.

10
11 34. (Original) The method of claim 27 wherein keys are generated in an
12 executable form which includes key information as well as code for decrypting
13 tickets using the key information.

14
15 35. (Original) The method of claim 27 wherein the keys are generated by
16 an authentication server, and are distributed to multiple login servers for providing
17 login tickets.

18
19 36. (Original) A computer readable medium having instructions stored
20 thereon for causing a computer to perform a method of updating keys used to decrypt
21 tickets used to log into multiple sites on a network, the method comprising:

22 generating a new key with a new version number to take the place of an old
23 key with an old version number;

24 storing the new key on a site to be logged into by a user;

25 changing a current key indication to the new key;

1 allowing current logged in users to continue using the old key; and
2 redirecting new users to a login server to obtain a ticket consistent with the
3 new key.

4

5 37. (Currently Amended) A method of logging on to multiple sites, the
6 method comprising:

7 sending a first login ticket to a desired site, wherein the login ticket is
8 encrypted to be decoded by a first key having a first version number;

9 receiving an indication that the first key has expired;

10 obtaining a second login ticket from an authentication server, wherein the
11 second login ticket is encrypted consistently with a new key having a second version
12 number; and

13 sending the second login ticket to the site to log into the site;

14 wherein said tickets are configured to enable a user to access and use one or
15 more affiliated servers without requiring any additional authentication information
16 other than authentication information originally provided by the user to an
17 authentication server.

18

19 38. (Original) The method of claim 37 wherein the tickets contain a
20 version number which is readable without decryption.

21

22 39. (Original) The method of claim 38 wherein the version number is a
23 one digit Hex 5 integer.

1 40. (Original) The method of claim 38 wherein the encrypted ticket
2 comprises an unencrypted version number, and encrypted information sufficient to
3 log a user into a desired site.

4

5 41. (Currently Amended) A computer readable medium having
6 instructions stored thereon for causing a computer to perform a method of logging on
7 to multiple sites, the method comprising:

8 sending a first login ticket to a desired site, wherein the login ticket is
9 encrypted to be decoded by a first key having a first version number;

10 receiving an indication that the first key has expired;

11 obtaining a second login ticket from an authentication server, wherein
12 the second login ticket is encrypted consistently with a new key having a second
13 version number; and

14 sending the second login ticket to the site to log into the site;

15 wherein said tickets are configured to enable a user to access and use one or
16 more affiliated servers without requiring any additional authentication information
17 other than authentication information originally provided by the user to an
18 authentication server.

19

20 42. (Currently Amended) An encrypted ticket for use in logging on to a
21 website, the ticket comprising:

22 an unencrypted version number corresponding to a key version number stored
23 on the website; and

1 an encrypted string identifying the website and information, which when
2 decrypted using the key having the same version number authenticates the user for
3 logging the user into the website;

4 wherein said ticket is configured to enable a user to access and use one or
5 more affiliated servers without requiring any additional authentication information
6 other than authentication information originally provided by the user to an
7 authentication server.

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25